resilience

REPORT

Cyber risk in higher education

What the claims data reveals about a structurally exposed sector

Cyber risk in higher education

What the claims data reveals about a structurally exposed sector

Introduction

Universities have a structural exposure most sectors don't share: deep reliance on shared platforms, decentralized operations across dozens of departments, and significant financial flows that are difficult to control centrally.

The external data reflects this. The largest higher ed data exposures of 2025 and 2026 all trace back to shared platform and vendor compromises, not direct attacks on institutions.[1] Ransomware attacks against colleges and universities jumped roughly 23% year over year in the first half of 2025, and education was the most commonly targeted sector for known exploited vulnerabilities in 2023, accounting for more than half of observed exploitation incidents that year.[2,3] In the UK, more than 90% of universities reported experiencing a breach or attack from April 2024 to April 2026, far outpacing the rate seen in most other sectors.[4]

This report draws on Resilience's portfolio of claims across higher education institutions spanning January 2021 through June 2026 to illustrate that exposure clearly, covering both the systemic risks that flow from how universities are built and the direct losses that reflect the financial and operational complexity of running one. Trend analysis uses a January 2022 through June 2026 window; the full dataset, including 2021 claims, informs the broader portfolio context.

Higher ed's structural problem is shared infrastructure

In 2025, while the frequency of attacks on the education sector held steady, severity climbed. Breached records rose 27% to 3.96 million, driven by larger third-party blast radius rather than more attacks.[1] The Resilience claims data shows where that concentration sits: higher education institutions share infrastructure in ways that multiply downstream exposure when a single vendor or platform is compromised. The two sections that follow show exactly how that played out in 2026 and 2023.

Across the January 2022 through June 2026 trend window (excluding a single, widely reported vendor incident discussed below), higher education sees roughly 50% more vendor and third-party incidents than the all-industry average: 35% of higher ed claims were triggered by a vendor or third-party event, compared to 24% for the rest of the Resilience portfolio.

This number reflects how higher ed is built. Institutions share platforms, clearinghouses, retirement systems, student health providers, and enrollment services with hundreds of other universities simultaneously. A single clearinghouse compromise can touch hundreds of institutions at once.

In 2026, the shared-platform risk materializes again

Three years later, the same dynamic played out again, at a different vendor. In spring 2026, Canvas, a widely used ed tech platform serving more than 8,800 institutions globally, was compromised via an exploited security vulnerability. The breach exposed approximately 275 million records across that base.[5]

This wasn't a case of individual institutions failing to secure their own environments. The platform is a shared dependency. A single vulnerability exposed thousands of institutions downstream, none of which could see it or do anything about it.

Roughly half of the higher education institutions in the Resilience portfolio were affected. To date, the attack has not generated significant immediate losses for the institutions involved; the potential for business interruption was contained and no data extortion has materialized. The longer-term exposure may come from downstream third-party litigation, which typically takes months to materialize after an incident of this scale.

MONDAY-MORNING TAKEAWAY

Higher ed security leaders should be asking which of their other shared EdTech and service provider dependencies carry the same concentration profile. And whether their third-party risk management program is built to surface that exposure before a threat actor finds it first.

Cl0p and the 2023 MOVEit wave

The pattern shows up clearly in 2023. Vendor-driven claims spiked to 61% of all higher ed claims in the Resilience portfolio that year, the highest share in the dataset.

What drove the spike? Higher education is the single largest sector in the Resilience portfolio tagged with the MOVEit event code, ahead of finance and insurance. All are vendor data breach claims, all closed, nearly all filed in 2023, consistent with the MOVEit mass-exploitation timeline of May through June 2023. A significant share of affected institutions appear more than once because multiple vendors in the MOVEit blast radius notified the same school separately. In one case, a single institution received separate notifications from four distinct vendors, each independently disclosing MOVEit exposure. The volume reflects how many separate downstream vendors in the supply chain touched each institution.[5,6]

None of these universities ran MOVEit directly. They were downstream of service providers who did: enrollment clearinghouses, retirement administrators, student health insurers, each serving thousands of institutions simultaneously. One exploited vulnerability cascaded through the sector.

External reporting confirmed approximately 900 colleges and universities were affected via National Student Clearinghouse alone.[7]

The direct loss picture when the threat is internal

When you strip out vendor events, the losses look different. The direct loss profile in higher ed is shaped less by ransomware than by the financial and operational complexity of running a university.

Among categorized non-vendor claims (January 2022 through June 2026, excluding vendor-driven events and uncategorized claims), the top four sources of claims cluster between 11% and 12%: email compromise at 12%, insider error at 12%, transfer fraud at 12%, and wrongful data collection at 11%. Direct ransomware sits at 8.5%.

Transfer fraud

Universities handle significant financial flows, including but not limited to financial aid disbursements, research grant management, tuition processing, and vendor payments — all high-value, high-volume, and often managed by decentralized departments with varying levels of controls.[9,10]

The governance around financial transactions varies widely across a university. A department managing a $1M construction contract operates under different controls than a central accounts payable team, and the people processing payments in decentralized units may have no exposure to business email compromise (BEC) training at all. Contract details are often public record, the amounts are predictable, and that combination makes universities a natural target for payment diversion.

For example, Unit 42, the threat intelligence and incident response arm of Palo Alto Networks, reported that BEC accounted for 34% of cases it investigated in 2023, with an average financial loss of $286,000 per successful wire fraud.[12]

Wrongful data collection

Wrongful data collection accounts for 11% of categorized non-vendor higher ed claims in the current trend window, and 78% of that volume concentrates in H1 2026. This is a new pattern in the dataset. The cause of loss typically involves allegations that an institution collected, stored, or shared personal data in ways that exceeded consent or violated applicable privacy requirements. For higher education, where student data flows through dozens of systems and departments under varying interpretations of FERPA, the exposure is structural. This finding warrants close monitoring as 2026 claims mature.

Insider error

Universities employ a large, frequently rotating workforce (faculty, staff, graduate students, administrators), many with access to sensitive data and varying levels of security training.[13]

In New York State alone, 200 of the 384 student data incidents reported to the New York State Education Department (NYSED) in 2024 were caused by human error (more than half).[14] The Family Educational Rights and Privacy Act (FERPA) imposes broad data protection obligations on institutions but includes no training requirements for those handling student data, leaving the people most likely to cause an incident with the least preparation to avoid one.

Mismailing — sending sensitive records to the wrong recipient — accounts for 7% of higher ed insider error claims and represents the kind of routine data handling failure that recurs wherever student records flow through multiple hands without consistent protocols.[15]

Ransomware

Direct ransomware accounts for 8.5% of categorized non-vendor higher ed claims (2022–H1 2026, excluding Canvas). The more significant ransomware exposure in this sector is vendor-mediated. Across the full higher ed portfolio, Vendor Data Breach accounts for 27% of all claims and Ransomware Impacting Vendor accounts for 16%, making them the two largest sources of claims by a wide margin. Canvas generated a high volume of claims but minimal financial losses to date; the 2023 MOVEit wave produced fewer claims but higher severity per incident. The direct ransomware percentage understates the sector's actual ransomware exposure because most of it flows through vendor events rather than hitting institutions directly.

CASE STUDY

Ransomware response

A prominent higher education institution took a severe ransomware hit — operations disrupted, sensitive data at risk, regulatory compliance in question. The attack had been enabled in part by end-of-life systems that hadn't been fully retired. Through the programs Resilience supports, the institution had access to a coordinated response: forensic investigation, legal and regulatory counsel, ransomware negotiation, and remediation work targeting the end-of-life systems that contributed to the exposure. In this case, the institution limited operational downtime and contained the incident before sensitive data was released.

What the outcome depended on was the speed and coordination of what came after. A continuous monitoring program is designed to surface end-of-life exposure like this before a threat actor can find it.

Tail risks worth naming

Repeat exposure at the institutional level

The institutions that file the most claims in the portfolio are not outliers who got unlucky once. They file across three and four consecutive years. Higher education's risk isn't episodic. The same structural vulnerabilities that generate one claim tend to generate the next one.

CASE STUDY

Incident resilience (education)

An education-sector client came to Resilience with two prior cyber incidents on record — the kind of loss history many underwriters won't take on. With support from Resilience's risk management programs, the client built a cyber hygiene plan with the controls associated with stronger ransomware terms — vulnerability monitoring, gap remediation, monthly engagements — and constructed and tested an incident response plan through tabletop exercises. When the client experienced another incident shortly after, they resolved it within days with no material loss.

The underlying gap — no tested plan, no remediation program — was the thread running through all of them. Once that changed, so did the outcome.

Copyright infringement

Copyright infringement accounts for roughly one in 19 non-vendor higher ed claims. Sector-specific, and essentially absent from most other industries in the portfolio at this rate. IT Services (6.0%) and Real Estate (5.1%) run higher by percentage; higher ed sits at 3.4% of its own claims but leads the portfolio by raw count.

So what's going on here? A closer look reveals that universities tend to use unlicensed third-party media in university marketing and communications — stock photos on websites, copyrighted music in social media videos, brand mark infringement. IP rights holders are also increasingly monitoring university content for unlicensed use, some systematically, which was a small but notable pattern in the claims data.

The sector-level pattern has a public-record analog. In March 2025, Sony Music and seven affiliated labels filed suit against a major research university, alleging the institution used more than 170 copyrighted songs in over 250 videos across 30 social media accounts without licenses, despite having been notified of the unauthorized use since 2021. Sony sought up to $150,000 per infringed work in statutory damages.[16] The case attracted sector-wide attention.[17]

MONDAY-MORNING TAKEAWAY

Universities produce a high volume of marketing content across decentralized departments — athletics, admissions, student organizations, academic units — without the licensing infrastructure a corporate marketing team would typically have. A periodic audit of media assets across social channels costs less than a single demand letter.

What this means for higher ed security leaders

The risk to universities is rarely direct, and that has a practical consequence. Third-party exposure is harder to monitor and harder to address through vendor contracts than a direct attack, but it's where the actual claims volume is concentrated.

For higher ed CISOs, the question has moved past whether a vendor incident will affect them. The question now is whether they have mapped their third-party exposure well enough to respond when it does. And whether their contracts and coverage reflect that exposure.

Direct losses are a different problem. Transfer fraud, insider error, and email compromise are largely preventable with controls that are well understood but inconsistently implemented across decentralized university structures. The controls exist. Most universities know where the training gaps are. What they haven't solved is getting consistent implementation across departments that operate with significant autonomy.

Where to start with third-party risk in higher ed

The starting point for a third-party risk management (TPRM) program in higher education should be a map of which shared platforms and service providers support your most critical functions. Chuck Norton, Senior Technical Security Advisor at Resilience, frames it this way: "You have a service portfolio of everything your organization delivers. Map vendors to those services. If admitting students is critical, identify which vendors support those functions, then tier accordingly."

For higher ed, that exercise quickly surfaces a small number of shared EdTech platforms and enrollment clearinghouses that simultaneously touch hundreds of other institutions. The concentration doesn't stem from a policy failure. It's a structural feature of how higher education is organized. But knowing which dependencies carry that profile is what separates institutions that can respond to a vendor incident in hours from those still trying to identify their exposure days later.

One further wrinkle: the risk in higher ed is often nth-party, not third-party. The 2023 MOVEit impact reached universities not through their direct vendors but through their vendors' vendors: retirement administrators and enrollment clearinghouses that used a file transfer tool the universities had never contracted with or assessed. A TPRM program that only looks one level deep will miss this. For a practical framework on vendor discovery, tiering, and implementation, see Resilience's TPRM series at cyberresilience.com/threatonomics.

Methodology

Resilience's proprietary data is drawn from the higher education cyber insurance claims portfolio. The dataset spans 2021 through 2026. Trend analysis covers January 2022 through June 2026. Claims associated with the Canvas vendor incident in spring 2026 have been excluded from trend analysis because the volume of claims from a single event would otherwise distort the frequency picture; the Canvas incident generated a high number of claims but minimal financial losses to date. Canvas is discussed separately where relevant. Analysis includes cause-of-loss classification, vendor attribution, and point-of-failure identification. Financial severity data is not included in this report due to insufficient population for meaningful analysis. All case studies are anonymized. Findings represent the Resilience higher education portfolio and should not be interpreted as representative of the broader higher education sector.

Endnotes

[1] Comparitech / GovTech, "Cyber Attacks on Schools Plateaued in 2025, but More Records Exposed," February 2026. Third-party software vulnerabilities drove the largest higher ed data exposures of 2025; 3.9 million records exposed across confirmed attacks, a 27% increase over 2024.

https://www.govtech.com/education/cyber-attacks-on-schools-plateaued-in-2025-but-more-records-exposed

[2] Times Higher Education / Comparitech, "Cybersecurity Threats to Universities and Colleges," January 2026. Ransomware attacks against colleges and universities jumped approximately 23% year over year in the first half of 2025, with around 130 confirmed incidents.

https://www.timeshighereducation.com/campus/cybersecurity-threats-universities-and-colleges-how-stay-safe

[3] Bitsight, "Top 10 Cyber Threats Facing the Education Sector in 2025," September 2025. Education was the most commonly targeted industry for Known Exploited Vulnerabilities (KEVs) in 2023, accounting for 54.3% of observed incidents.

https://www.bitsight.com/blog/top-10-cyber-threats-facing-education-sector

[4] UK Department for Science, Innovation & Technology, "Cyber Security Breaches Survey 2025/2026: Education Institutions Findings," April 2026. More than 90% of UK universities reported a breach or attack in the past 12 months.

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings

[5] Jessica Lyons, "Double Canvas intrusion confirmed as ShinyHunters resets leak deadline," The Register, May 12, 2026. ShinyHunters claimed approximately 3.65 TB of data, including roughly 275 million records from approximately 8,800 schools.

https://www.theregister.com/security/2026/05/12/double-canvas-intrusion-confirmed-as-shinyhunters-resets-leak-deadline/5238361

[6] Anna Merod, "What to watch for as the MOVEit breach hits higher ed," Higher Ed Dive, July 13, 2023. Confirms higher ed disproportionately hit via shared service providers. Notes TIAA was compromised via its vendor PBI Research Services, not through direct MOVEit use.

https://www.highereddive.com/news/moveit-breach-colleges-university-higher-ed/686592/

[7] Natalie Schwartz, "MOVEit breach hit nearly 900 colleges, says National Student Clearinghouse," Higher Ed Dive, September 27, 2023. TIAA confirmed one of its third-party vendors (PBI Research Services) was compromised via MOVEit; multiple institutions confirmed they were affected by both the TIAA and NSC breaches.

https://www.highereddive.com/news/move-it-900-colleges-breach/694835/

[8] "MOVEit fallout continues as National Student Clearinghouse says nearly 900 schools affected," The Record (Recorded Future News), September 25, 2023. NSC confirmed nearly 900 colleges and universities had data stolen; NSC serves approximately 3,600 North American colleges and universities.

https://therecord.media/moveit-fallout-continues-nsc-schools

[9] USAFacts, "How universities spend billions in government funds," May 2025. In FY2023, federal agencies funded $59.6 billion of university R&D expenses. Cornell University's grant and contract revenue totaled $1.059 billion in FY2025.

https://usafacts.org/articles/what-do-universities-do-with-the-billions-they-receive-from-the-government/

[10] Houston Community College, "Understanding and Preventing Fraud in Higher Education," presentation, November 20, 2024.

https://www.hccs.edu/media/houston-community-college/district/pdf/Fraud-Awareness-Presentation-Final---11-20-2024-(2).pdf

[11] University of California Riverside ITS, "University Loses $1.9 Million After Falling Victim to Business Email Compromise," April 24, 2024. Documents Southern Oregon University BEC: attackers spoofed a construction contractor and diverted a $1.9M wire payment.

https://its.ucr.edu/attack-alerts/2024/04/24/university-loses-19-million-after-falling-victim-business-email-compromise

[12] Palo Alto Networks / Unit 42, "What Is Business Email Compromise (BEC)?" 2024. BEC: 34% of Unit 42 cases in 2023; avg. $286K loss per successful wire fraud. FBI IC3: 73% of all reported cyber incidents in 2024 attributed to BEC; $55B+ cumulative losses over the past decade.

https://www.paloaltonetworks.com/cyberpedia/what-is-business-email-compromise-bec-tactics-and-prevention

[13] CampusGuard, "Student Workers: Protecting Sensitive Data," January 2025. Documents recurring onboarding gap: institutions can generally expect high turnover and often need to train a new group of student workers each term.

https://campusguard.com/post/student-workers-protecting-sensitive-data/

[14] Public Interest Privacy Center, "Fixing FERPA: Adding Cybersecurity Requirements," July 2025. In New York State, 200 of 384 student data incidents reported in 2024 were caused by human error. Notes FERPA includes no training requirements for those handling student data.

https://publicinterestprivacy.org/fixing-ferpa-cybersecurity/

[15] EdTech Magazine, "Shadow Data in Higher Education: Governing Unsanctioned Data Before It Becomes a FERPA Problem," March 6, 2026. Documents faculty and staff downloading student records into personal spreadsheets or unsanctioned cloud tools; FERPA liability follows the data regardless of where it is stored.

https://edtechmagazine.com/higher/article/2026/03/shadow-data-higher-education-governing-unsanctioned-data-it-becomes-ferpa-problem-perfcon

[16] ArentFox Schiff, "USC Faces the Music: Sony Music Sues USC for Unauthorized Use of Sound Recordings in Social Media," March 26, 2025; Cullen & Dykman LLP, "Copyright Meets Campus," July 1, 2025. Sony Music and seven affiliated labels alleged USC used 170+ copyrighted songs in 250+ videos across 30 social media accounts without licenses despite notification since 2021. Statutory damages sought: up to $150,000 per work.

https://www.afslaw.com/perspectives/alerts/usc-faces-the-music-sony-music-sues-usc-unauthorized-use-sound-recordings

https://www.cullenllp.com/blog/copyright-meets-campus-sony-sues-usc-for-unlicensed-music-on-social-media/

[17] University of Arkansas, "Annual Copyright Infringement Notice," October 3, 2025. Cites Sony/USC suit as a sector-wide caution.

https://news.uark.edu/articles/80125/annual-copyright-infringement-notice